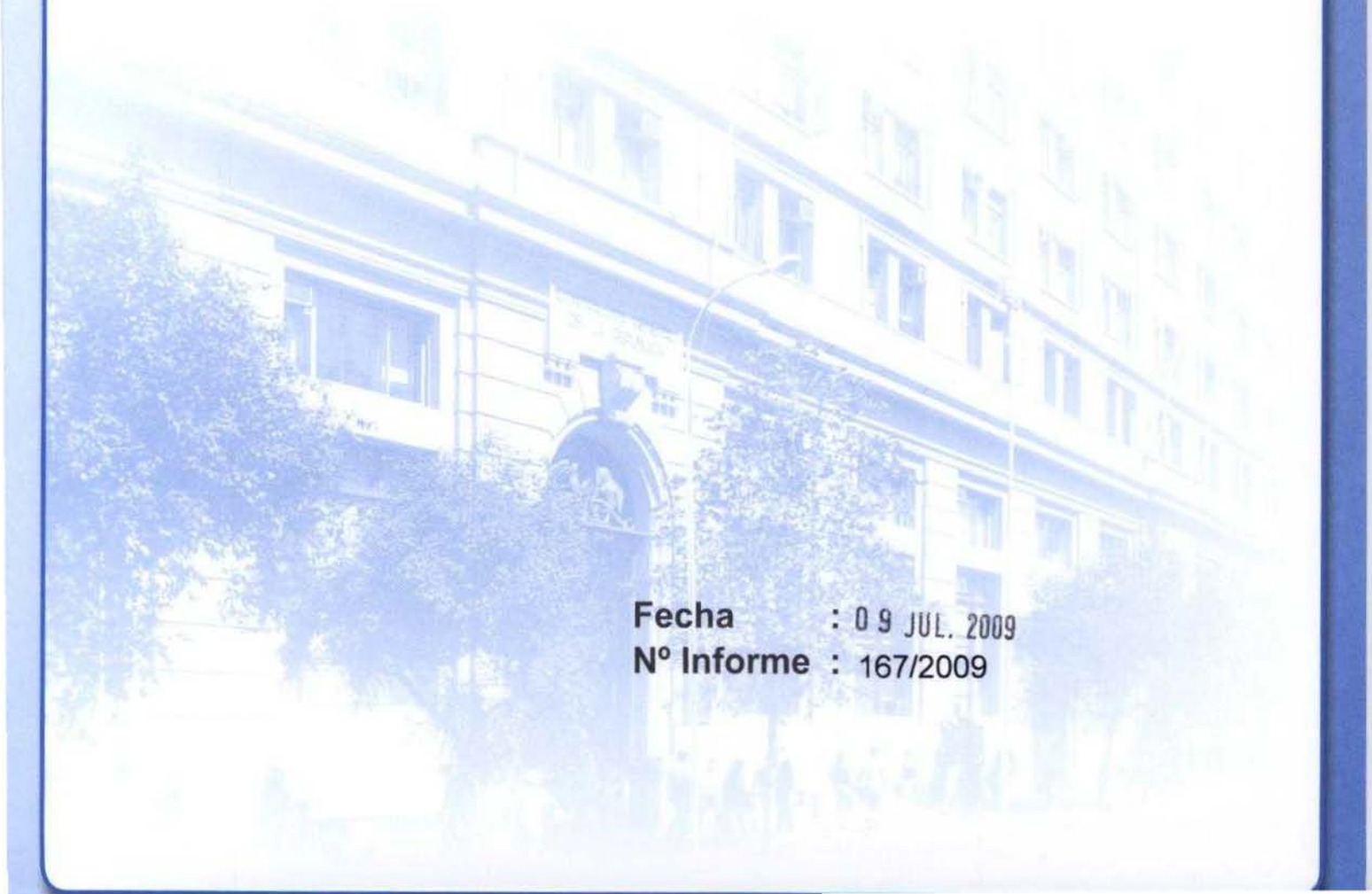
CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE MUNICIPALIDADES

Informe Final Municipalidad de Maipú



Fecha : 09 JUL. 2009
Nº Informe : 167/2009

CONTRALORÍA GENERAL DE LA REPÚBLICA

DIVISIÓN DE MUNICIPALIDADES
SUBDIVISIÓN DE AUDITORÍA E INSPECCIÓN
ÁREA DE AUDITORÍA 1

REF.: 7.075/09
DMSAI 120/09

REMITE INFORME FINAL QUE INDICA

SANTIAGO, 09. JUL 2009. 036418

Adjunto sírvase encontrar copia del Informe Final N° 167 debidamente aprobado, sobre Auditoría de Sistemas Informáticos efectuada en el Servicio Municipal de Agua Potable y Alcantarillado en esa Municipalidad.

Saluda atentamente a Usted,

Por Orden del Contralor General
PRISCILA JARA FUENTES
Abogado
Subjefe División de Municipalidades

AL SEÑOR
ALCALDE DE LA
MUNICIPALIDAD DE
MAIPÚ

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA

DIVISIÓN DE MUNICIPALIDADES
SUBDIVISIÓN DE AUDITORÍA E INSPECCIÓN
ÁREA DE AUDITORÍA 1

REF.: 7.075/09
DMSAI 120/09

REMITE INFORME FINAL QUE INDICA

SANTIAGO, 09. JUL 2009. 036419

Adjunto, sírvase encontrar copia del Informe Final DMSAI Nº 120 de 2009, de esta Contraloría General, con el fin de que, en la primera sesión que celebre el Concejo Municipal, desde la fecha de su recepción, se sirva ponerlo en conocimiento de ese Órgano Colegiado entregándole copia de los mismos.

Al respecto, Ud. deberá acreditar ante esta Contraloría General, en su calidad de Secretario del Concejo y ministro de fe, el cumplimiento de este trámite dentro del plazo de diez días de efectuada esa sesión.

Saluda atentamente a Usted,

Por Orden del Contralor General
PRISCILA JARA FUENTES
Abogado
Subjefe División de Municipalidades

AL SEÑOR
SECRETARIO MUNICIPAL DE
MAIPÚ

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE MUNICIPALIDADES
SUBDIVISIÓN DE AUDITORÍA E INSPECCIÓN
DEPARTAMENTO DE AUDITORÍA

REF. N° 7.075/09
DMSAI. N° 120/09
A.T. N° 146/09

INFORME FINAL SOBRE DE AUDITORÍA DE SISTEMAS INFORMÁTICOS EFECTUADA EN EL SERVICIO MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE MAIPÚ - SMAPA.

SANTIAGO, 09 JUL. 2009

En cumplimiento del Plan Anual de Fiscalización aprobado por este Organismo de Control y de acuerdo con las facultades establecidas en la Ley 10.336, Orgánica de esta Institución, se realizó una auditoría de tecnologías de información en el Servicio Municipal de Agua Potable y Alcantarillado de Maipú, SMAPA.

OBJETIVO.

Verificar los controles en el procesamiento de datos; en el mantenimiento de la plataforma de software, hardware y servicios automáticos; y, en el cumplimiento de los contratos de desarrollo de sistemas, servicios informáticos, arriendo y/o compra de equipamiento y compra de insumos.

METODOLOGÍA.

La revisión fue practicada en conformidad con normas y procedimientos aceptados por la Contraloría General, por lo tanto, incluyó las pruebas de validación y otros medios técnicos considerados necesarios en las circunstancias.

UNIVERSO FISCALIZADO.

La revisión abarcó el período comprendido entre enero de 2007 y el primer trimestre de 2008, para el cual se analizó los aspectos relativos a las tecnologías de información del citado servicio.

La revisión, en términos generales, consistió en el análisis de los contratos informáticos, las políticas informáticas, los métodos de integridad de datos, los recursos informáticos, la validez de la información, las salvaguardas de activos informáticos y la efectividad de la aplicación de controles.

Contralor General de la República

A LA SEÑORA
SUBJEFE DE LA DIVISIÓN DE MUNICIPALIDADES
P R E S E N T E.
JPTV/

MUESTRA EXAMINADA.

La revisión se efectuó sobre el 100% de las actividades del período señalado.

Cabe precisar que, con carácter confidencial, mediante oficio N° 58.955, de 15 de diciembre de 2008, fueron puestas en conocimiento del alcalde las observaciones comprobadas al término de la visita, con la finalidad que formulara los alcances y precisiones que, a su juicio, procedieran, lo que se concretó mediante oficio N° 1000/005, de 6 de febrero de 2009.

El análisis de las observaciones formuladas en el citado Preinforme, en conjunto con los antecedentes aportados por la autoridad edilicia en su respuesta, determinaron lo siguiente:

1.- ORGANIZACIÓN.

1.1.- Estructura funcional, jerárquica y personal del área informática.

Se observó, inicialmente, la ausencia de planes de capacitación periódica que permitieran el desarrollo del personal informático en las nuevas tecnologías existentes y el análisis de soluciones que permitan mejorar la gestión.

En su respuesta, la autoridad comunal indica ello no es efectivo lo observado, por cuanto existe capacitación y se enmarca en lo establecido por la Subdirección de Recursos Humanos. Agrega, que durante el año 2008 fueron capacitados doce funcionarios de la Dirección de Tecnología y Comunicaciones - DITEC - en un curso de Active Directory, software para la administración de equipos basado en políticas institucionales y que, además, se capacitó a tres técnicos en Administración de la Plataforma Exchange 2003 Server, para el manejo del correo institucional. Agrega que, debido a los alcances de este Organismo, se instruyó que durante el año 2009 se incluya en el plan de capacitaciones de la Subdirección de Recursos Humanos, otras capacitaciones específicas que permitan mejorar la gestión de la DITEC y, por ende, la calidad de sus servicios a los usuarios municipales.

Al respecto, cabe precisar, que la observación realizada se efectuó sobre el período auditado, para el cual se carecía, además, de un plan de capacitación; en todo caso, en base a los antecedentes aportados, se levanta la observación formulada.

1.2.- Recursos de plataforma Software y Hardware.

No se dispone de regulaciones para crear y operar procedimientos de operación de sistemas, bases de datos y plataforma de software general. No se encuentran regulados planes de contingencia y continuidad, que garanticen el buen funcionamiento de los sistemas y permitan identificar los riesgos asociados, dado que no existen áreas de especialización que distribuyan la carga de operaciones informáticas diarias.

En la respuesta se indica que se ha instruido a la DITEC para que implemente procedimientos escritos y planes de contingencia, respaldo de información, manejo de base de datos y de hardware de usuarios.

Las medidas dispuestas por esa autoridad comunal permitirán subsanar las observaciones formuladas, en la medida que se concreten efectivamente, lo que se verificará en futuras fiscalizaciones.

1.3.- Aplicaciones.

Se advirtió la ausencia de respaldos de perfiles de sistemas operativos y procedimientos formales de actualización de parches de sistema operativo y de aplicaciones de oficina.

Asimismo, se realizó un análisis mediante diagramas de flujos de datos y diagramas de entidad - relación de los procesos de SGC SMAPA, facturación, recaudación, subsidio, tarificación, contabilidad, cobranza, medición y sistemas en línea, cuyos módulos fueron evaluados como de mayor riesgo. Además, se llevaron a cabo pruebas de validación de entradas y salidas de los registros de dichos procesos, determinando que los módulos de aplicaciones cumplen las funcionalidades de mantención, operación y registro de los datos, por lo anterior no se formuló observaciones a este respecto.

Sobre los respaldos de perfiles de sistemas, en la respuesta de la autoridad se informa que, por la cantidad de equipos no es posible físicamente realizar el procedimiento, sin embargo, se ha establecido un sistema de soporte que asiste en caso de que un usuario requiera respaldar la información que el equipo contenga. Agrega que el perfil que contiene el sistema operativo se traspasa automáticamente al nuevo equipo y, en caso de daño físico a los dispositivos de almacenamiento, operan las herramientas de rescate que cuentan con tasa de recuperabilidad de 98%.

En cuanto a los procedimientos de parches de los sistemas operativos y aplicaciones de oficina, se establece la restricción en el uso de los equipos por parte de los usuarios, que impide la instalación de software o modificación de configuraciones del sistema, dejando está última facultad al Administrador de los Sistemas. Finalmente, sobre la falta de licenciamiento de la plataforma de servidor de correo electrónico Exchange 2003 Server, se informa el inicio de comunicaciones con la empresa proveedora con el fin de regularizar la situación.

Lo señalado en los párrafos precedentes no permite subsanar completamente las observaciones advertidas, cuya regularización definitiva se verificará en una próxima fiscalización.

2.- SALA DE LA UNIDAD INFORMÁTICA.

La citada sala cumple sólo parcialmente con las condiciones necesarias para el resguardo de los datos. En efecto, la configuración de la red eléctrica y de datos conlleva el riesgo de afectar la integridad de la información existente, puesto que no se encuentra certificada en su totalidad, dado su crecimiento inorgánico. Además, se estableció la ausencia de un sistema de detección, control y extinción de incendio y, de detección de cambios de estado ambiental con puntos de monitoreo.

Por su parte, el sistema de aire acondicionado de precisión no posee un microprocesador que indique los intervalos del servicio y las horas de operación del sistema, no encontrándose certificado para el uso en la sala de servidores. No se cuenta con alarmas específicas y sistemas de alerta en caso de siniestro, como inundaciones y sismos, entre otros, ni hay señalética de seguridad en las instalaciones.

Asimismo, en la actualidad no se aplican en las operaciones, medidas de mitigación de riesgos de fallas en la plataforma de software y hardware. La disposición del equipamiento impide la correcta mantención y resulta ineficiente respecto de la utilización del rack de distribución de cables de datos, de energía y de comunicaciones.

En la respuesta de la autoridad se señala que actualmente el Data Center es un recinto cerrado, con acceso controlado, iluminación de emergencia, extintores y servicio ininterrumpido de electricidad para los equipos y que el recinto cuenta con corriente eléctrica trifásica para mayor estabilidad contra las alzas de voltaje, lo que se traduce en protección para el equipamiento. Señala, también, que el Data Center cuenta con circuito cerrado de televisión que graba y transforma el material a digitar, pudiendo visualizarse a través de Internet. Finalmente, se encuentran instalados dos equipos de aire acondicionado de 45.000 y 20.000 BTU con autopartida ante corte eléctrico y sensor de temperatura constante.

Agrega, que aún habiéndose realizado mejoras en los últimos meses, se ha instruido a la DITEC disponer la elaboración de un plan de acción y mejoramiento calendarizado, que se presentará para aprobación de SMAPA y de la Administración Municipal.

En base a los antecedentes aportados, se levantan las observaciones formuladas, sin perjuicio de las verificaciones futuras que se efectúen.

3.- SEGURIDAD DE LA INFORMACIÓN.

Se advirtió la inexistencia de políticas y procedimientos de registro de personal en tránsito dentro de las instalaciones informáticas, tanto interno como externo de empresas contratistas o que prestan servicios regulados por contrato. Además, no existe personal de seguridad o sistemas de vigilancia remota para el control de las instalaciones de la Unidad de Informática y no se documentan los procedimientos de cambios de datos o configuración que se realizan en equipos de la sala de servidores.

Tampoco existen normativas formales de administración y seguridad aplicadas por parte de los usuarios finales de los sistemas, en cuanto a realizar cambios de claves en forma periódica.

Asimismo, se verificó la ausencia de duplicación de datos en servidor externo a las instalaciones de SMAPA, como una medida de resguardo para la continuidad del servicio y que, no se ha contratado un soporte continuo.

Por otra parte, se requiere de una redefinición de tipos y tiempos de interrupción en las operaciones de los sistemas, teniendo en consideración período y cantidad de minutos que se estimen aceptables. Además, se verificó la inexistencia de medidas de seguridad física de los datos, no existiendo respaldos de datos en sitios secundarios o el resguardo en una caja de seguridad con acceso a través de llave, tarjeta magnética o duplicación de respaldos para conservar disponibilidad de servicios.

En la respuesta se indica que los servidores se encuentran físicamente en el Data Center de DITEC y que la información es respaldada externamente mediante un proceso que considera, además, restauración de los medios a través de la empresa AQB. Adicionalmente, en el mes de febrero del año 2008 se constituyó el Comité de Seguridad de la DITEC para establecer mecanismos de seguridad a nivel institucional y se instruyó el establecimiento de medidas de mejoramiento para dar solución a las observaciones planteadas en el Preinforme de esta entidad.

En relación con lo anterior, debe precisarse que los antecedentes proporcionados en su oportunidad no se ajustan exactamente al período de ejecución de la auditoría, lo que generó una inexactitud en las observaciones, de modo que la revisión de estos aspectos será considerada en una próxima auditoría sobre la materia.

4.- BASE DE DATOS.

Conforme con la información proporcionada durante la visita, los datos respaldados carecían de encriptación y verificación de integridad de información primaria, lo que aumenta el riesgo en la seguridad al momento de acceder a la información que se encuentra dentro de los respaldos. Además, los archivos de registros de transacciones (Log), no se usan para revisar la integridad del servicio ni se ha hecho una auditoría de los procesos para evaluar el rendimiento y la criticidad de las operaciones más recurrentes, así como la detección de intrusiones.

Se verificó la falta de procedimientos formales para eliminar información física de los medios de almacenamiento en los períodos de tiempo asignados. Asimismo, no se mantenían productos de la estructura de base de datos, manuales de sistemas y procesos, sino sólo los programas ejecutables y los servicios en línea, lo que determina que cualquier modificación a realizar debe ser planificada con antelación con la empresa proveedora, sin poder acceder a un conocimiento general, para optimizar los servicios de SMAPA.

Se determinó que no existían procedimientos de control para el cruce de datos entre los distintos sistemas y no se utilizaban herramientas externas para la administración de la base de datos, quedando en evidencia la existencias de una escasa cantidad de usuarios capacitados para administrar la base de datos.

En la respuesta se indica que la empresa AQB realiza la labor de encriptar los datos mediante el software Retrospect una vez que los datos son traspasados a cinta; no obstante ello, en el período auditado no se proveyó de información acerca de la existencia de un contrato de prestación de servicios con dicha empresa, encargada de la administración de los respaldos y restauraciones.

Se informa, también, que se utiliza el backup propietario de MS SQL Server 7.0 para realizar el respaldo de las bases de datos y,. en forma parcial, el software Bulkcopy y que por su parte, la empresa Sonda entregó manuales de procedimientos, operaciones y DFDs de los sistemas en explotación; sin embargo, en el período de fiscalización no se informó acerca de su uso, como constaba en el cuadro de aplicaciones y sistemas utilizados a nivel de empresa.

Además, se indica en la respuesta que para efectos de administración de la base de datos no se requiere una herramienta externa, puesto que el mismo software que maneja el sistema comercial la posee. Adicionalmente, el riesgo de seguridad para acceder a la información se ve resguardado mediante la comparación que realiza el área de contabilidad entre libro de ventas de SMAPA y el Sistema Cubo OLAP, que corresponde al procesamiento analítico en línea y que tiene por ventaja realizar consultas con una mayor velocidad de respuesta, puesto que en una base de datos relacional se almacenan entidades en tablas discretas si han sido normalizadas.

Respecto de la detección de intrusiones se cuenta con un sistema IDS que cuenta con un Firewall WatchGuard, que reporta posibles intrusiones detectadas en el enlace principal, sin embargo, se reconoce la falta de escrituración del procedimiento, por lo que se incluirán las observaciones en el plan de acción calendarizado a SMAPA y la Administración Municipal para su implantación.

Finalmente, la autoridad municipal señala que cuenta con manuales de procedimientos, operaciones y diagramas de flujos de datos de los sistemas; sin embargo, en el período en que se llevó a cabo la auditoria no se entregó información respecto de manuales de procedimientos y operaciones de los sistemas.

En consecuencia, considerando que parte de lo observado obedeció a la falta de entrega de antecedentes actualizados por esa entidad, la materia será objeto de futuras fiscalizaciones.

5.- REDES.

La normativa interna adolece de instrucciones para regular las extensiones de puntos de red, la ampliación de señal, los layout de rack y la administración de anchos de banda. Se verificó la omisión de procedimientos para el análisis de las vulnerabilidades de red municipal y la ausencia de identificación de los equipos computacionales y los respectivos usuarios propietarios que se encuentren conectados a la red.

En la respuesta se indica que se cuenta con un sistema de inventario Aranda que mantiene la identificación completa de los equipos conectados a la red y que, sin perjuicio de ello, se instruyó la adopción de medidas tendientes a dar solución a las observaciones e informar su implementación y avance a la Contraloría General.

Cabe hacer presente, que en el período fiscalizado no se informó acerca de la utilización del sistema de inventario Aranda que actualmente mantiene un registro de los equipos conectados.

En el entendido que se dispondrán las medidas señaladas, se levanta lo observado inicialmente, cuyo cumplimiento será objeto de futuras fiscalizaciones.

6.- POLÍTICAS Y REGLAS.

Se comprobó que al personal municipal no se le ha brindado instrucción respecto de la seguridad de las instalaciones y el equipamiento.

Asimismo, no se han establecido políticas específicas para la adquisición de licencias de software, la adopción de medidas de seguridad física para el uso de las instalaciones de la Unidad Informática, la aplicación de medidas de seguridad lógica y confidencialidad de la Información, el uso de los servicios de la red de datos institucional y de las cuentas de usuarios, la capacitación de personal informático, las normas de uso del servicio de Internet y del correo electrónico y los planes concretos de mantenimiento preventivo y correctivo de software de aplicaciones, hardware y telecomunicaciones.

Por otra parte, se determinó la falta de registros de incidentes que indiquen pérdidas de datos y/o alteraciones en el funcionamiento de los sistemas, bases de datos o instalaciones y de ranking con elementos críticos o pruebas de estado de plataforma seguridad para actualización (aplicación de norma ISO 27001).

La dirección desconoce los riesgos asociados al servicio prestado a clientes, riesgo de negocios y de parálisis de la gestión municipal. Además, no existe un plan de continuidad en los sistemas de información ni planes de capacitación en controles y seguridad de sistemas de información, como tampoco existen políticas normativas de grabación de datos de clientes. Respecto del layout de equipamiento físico, certificación de arquitectura de red e interconexión de dispositivos para administración de plataforma de equipos, datos y comunicaciones, se verificó la falta de planes de crecimiento de puntos red y equipos para abastecer las necesidades municipales.

En la respuesta de la autoridad comunal se informa que en los años 2005 y 2006, se realizaron encuentros sobre materias informáticas tales como Seguridad de la Información, con funcionarios municipales, por parte de DITEC y que, próximamente, se publicará un Boletín de Seguridad para ser distribuido al municipio; no obstante, los encuentros aludidos no corresponden al período fiscalizado.

Sobre la falta de políticas específicas, se informa que DITEC realizará un plan de acción calendarizado que incluirá todas las observaciones que a la fecha no se hayan subsanado y, que aún cuando no existan manuales de procedimientos sobre materias específicas, cada una de ellas son desarrolladas y aplicadas por personal profesional de la DITEC.

En base a los antecedentes aportados, se levanta la observación formulada, sin perjuicio de las verificaciones posteriores a realizar en futuras auditorías.

7.- EXAMEN DE CONTRATOS INFORMÁTICOS.

Existe un único contrato en estado de operación, suscrito con Sonda S.A., cuyo plazo de ejecución es de 36 meses a partir del 1 de abril de 2007. A su respecto se verificó la existencia de la boleta de garantía N° 99414, de 24 de abril de 2007, del Banco Bice, por un monto de $ 28.969.354.-, con vencimiento el 31 de mayo de 2010, todo ello de acuerdo con lo dispuesto en el respectivo convenio.

El contrato se encuentra normado técnicamente y en funcionamiento, realizándose pruebas de validación de integridad de datos a registros de procesos críticos, evaluación de disponibilidad, tiempo de respuesta y reportes de salida, sin que de dichas comprobaciones surgieran observaciones que formular.

Los pagos de los servicios se efectuaron conforme a lo pactado y se encontraban al día.

CONCLUSIONES:

1.- En mérito de lo expuesto, la autoridad deberá dar efectivo cumplimiento a las medidas enunciadas en los numerales 1.2; 1.3 y; 5 del presente informe, tendientes a solucionar las observaciones planteadas, cuya efectividad será comprobada en las próximas visitas que se realicen a la Entidad, conforme las políticas de este Organismo sobre seguimiento de los programas de fiscalización.

2.- Respecto de lo señalado en los puntos 3 y 4, cabe señalar que, considerando que en su oportunidad se dispuso de información que se encontraba en proceso de cambio, según se advierte de la respuesta al Preinforme respectivo, las observaciones inicialmente planteadas serán evaluadas en una próxima fiscalización.

Transcríbase al Alcalde y al Concejo Municipal de Maipú.

Saluda atentamente a Ud.

VIVIAN AVILA FIGUEROA
JEFA AREA AUDITORÍA
SUBDIVISIÓN AUDITORÍA E INSPECCIÓN
DIVISIÓN DE MUNICIPALIDADES

www.contraloria.cl